(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

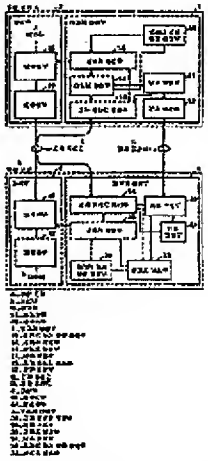
(11)Publication number: 1020060003329 A
(43)Date of publication of application:
10.01.2006

(21)Application number: 1020057016821
(22)Date of filing: 09.09.2005
(30)Priority: 10.03.2003 JP2003 2003063532

(51)Int. Cl H04L 9/12
H03M 13/09
H03M 13/19

(71)Applicant: MITSUBISHI ELECTRIC CORPORATION
(72)Inventor: MATSUMOTO WATARU
WATANABE YODAI

(54) QUANTUM KEY DELIVERY METHOD AND COMMUNICATION DEVICE



(57) Abstract:

A quantum key delivery method is a method for estimating original transmission data from reception data having probability information. For example, parity check matrix generation sections (10, 30) generate the same parity check matrixes and a syndrome generation section (14) notifies error correction information generated according to the parity check matrix and the transmission data to a communication device of the reception side via a public communication path. A syndrome decoding section (33) estimates the transmission data according to the error correction information and the reception data having the probability information. Furthermore, until the errors of the reception data are corrected completely, an error correction process is repeatedly executed by increasing the number of rows of the parity check matrix under a predetermined constraint condition.

Legal Status
Date of request for an examination (20050909)
Notification date of refusal decision ( )
Final disposal of an application (registration)
Date of final disposal of an application (20070517)
Patent registration number (1007424500000)
Date of registration (20070718)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent ( )
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )

(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[8]
H04L 9/12 (2006.01)
H03M 13/09 (2006.01)
H03M 13/19 (2006.01)

(11) 공개번호 10-2006-0003329
(43) 공개일자 2006년01월10일

(21) 출원번호 10-2005-7016821
(22) 출원일자 2005년09월09일
번역문 제출일자 2005년09월09일
(86) 국제출원번호 PCT/JP2004/003111
국제출원일자 2004년03월10일
(87) 국제공개번호 WO 2004/088915
국제공개일자 2004년10월14일

(30) 우선권주장 JP-P-2003-00063532 2003년03월10일 일본(JP)

(71) 출원인 미쓰비시덴키 가부시키가이샤
일본국 도쿄도 지요다쿠 마루노우치 2쵸메 7반 3고

(72) 발명자 마츠모토 와타루
일본 도쿄도 지요다쿠 마루노우치 2쵸메 2반 3고 미쓰비시덴키가부시키가이샤 내
와타나베 요다이
일본 사이타마켄 와코시 히로사와 2-1 도꾸리쯔교세이호징리가가쿠 겐큐소 내

(74) 대리인 김창세

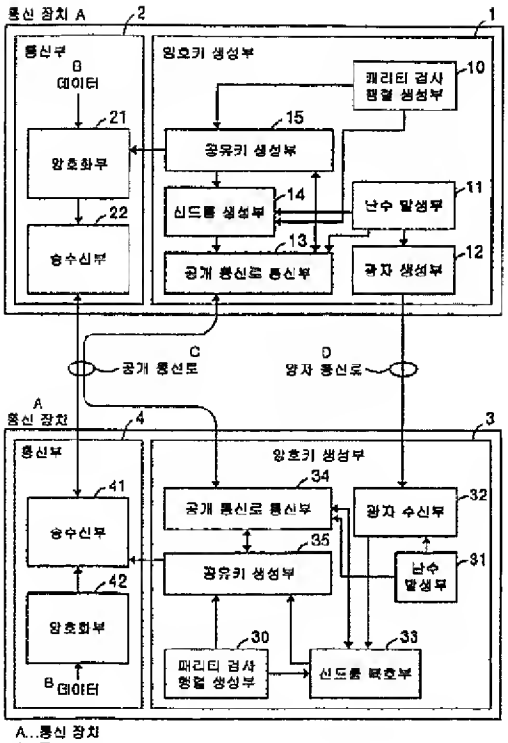
심사청구 : 있음

(54) 양자키 배송 방법 및 통신 장치

요약

본 발명의 양자키 배송 방법은, 확률 정보 첨부의 수신 데이터로부터 본래의 송신 데이터를 추정하는 방법으로서, 예컨대, 패리티 검사 행렬 생성부(10, 30)가, 동일한 패리티 검사 행렬을 생성하고, 신드롬 생성부(14)가, 상기 패리티 검사 행렬과 상기 송신 데이터에 근거하여 생성한 오류 정정 정보를, 공개 통신로를 거쳐 수신측의 통신 장치에 통지하고, 신드롬 복호부(33)가, 상기 오류 정정 정보 및 상기 확률 정보 첨부의 수신 데이터에 근거하여 상기 송신 데이터를 추정하고, 또한, 수신 데이터의 오류를 완전히 정정할 수 있을 때까지, 소정의 구속 조건하에서 패리티 검사 행렬의 행수를 증가시키면서 오류 정정 처리를 반복하여 실행하는 구성으로 했다.

대표도



A...통신 장치
2...통신부
B...데이터
21...암호화부
22...송수신부
1...암호키 생성부
10...패리티 검사 행렬 생성부
15...공유키 생성부
14...신드롬 생성부
11...난수 발생부
13...공개 통신로 통신부
12...광자 생성부
C...공개 통신로
D...양자 통신로
4...통신부
41...송수신부
42...암호화부
3...암호키 생성부
34...공개 통신로 통신부
32...광자 수신부
35...공유키 생성부
31...난수 발생부
30...패리티 검사 행렬 생성부
33...신드롬 복호부

발명의

기술분야

본 발명은 고도로 안전성이 보증된 공통키를 생성하는 것이 가능한 양자키 배송 방법에 관한 것이며, 특히, 오류 정정 부호를 이용하여 데이터 오류를 정정할 수 있는 양자키 배송 방법 및 당해 양자키 배송을 실현 가능한 통신 장치에 관한 것이다.

배경기술

이하, 종래의 양자 암호 시스템에 대하여 설명한다. 최근, 고속 대용량인 통신 기술로서 광통신이 널리 이용되고 있지만, 이러한 광통신 시스템에서는, 광의 온/오프로 통신이 행해지고, 온일 때에 대량의 광자가 송신되고 있기 때문에, 양자 효과가 직접 나타나는 통신계로는 되어 있지 않다.

한편, 양자 암호 시스템에서는, 통신 매체로서 광자를 이용하여, 불확정성 원리 등의 양자 효과가 발생하도록 1개의 광자로 1 비트의 정보를 전송한다. 이 때, 도청자가, 그 편광, 위상 등의 양자 상태를 모르고 적당히 기저를 선택하여 광자(光子)를 측정하면, 그 양자 상태에 변화가 발생한다. 따라서, 수신측에서는, 이 광자의 양자 상태의 변화를 확인함으로써, 전송 데이터가 도청됐는지 여부를 인식할 수 있다.

도 10은 종래의 편광을 이용한 양자키 배송의 개요를 나타내는 도면이다. 예컨대, 수평 수직 방향의 편광을 식별 가능한 측정기에서는, 양자 통신로 상의, 수평 방향(0°)으로 편광된 광과 수직 방향(90°)으로 편광된 광을 정확하게 식별한다. 한편, 경사 방향(45°, 135°)의 편광을 식별 가능한 측정기에서는, 양자 통신로 상의, 45° 방향으로 편광된 광과 135° 방향으로 편광된 광을 정확하게 식별한다.

이와 같이, 각 측정기는, 규정된 방향으로 편광된 광에 대해서는 정확하게 인식할 수 있지만, 예컨대, 경사 방향으로 편광된 광을 수평 수직 방향(0°, 90°)의 편광을 식별 가능한 측정기에 의해 측정하면, 수평 방향과 수직 방향으로 편광된 광을 각각 50%의 확률로 랜덤으로 식별한다. 즉, 식별 가능한 편광 방향에 대응하지 않는 측정기를 이용한 경우에는, 그 측정 결과를 해석하더라도, 편광된 방향을 정확하게 식별할 수가 없다.

도 10에 나타내는 종래의 양자키 배송에서는, 상기 불확정성(랜덤성)을 이용하여, 도청자에게 알려지지 않고 송신자와 수신자 사이에서 키를 공유한다(예컨대, Bennett, C. H. and Brassard, G.:Quantum Cryptography: Public Key Distribution and Coin Tossing, In Proceedings of IEEE Conference on Computers, System and Signal Processing, Bangalore, India, pp.175-179(DEC.1984) 참조). 또, 송신자 및 수신자는 양자 통신로 이외에 공개 통신로를 사용할 수 있다.

여기서, 키의 공유 수순에 대하여 설명한다. 우선, 송신자는, 난수열(1, 0의 열: 송신 데이터)을 발생시키고, 또한 송신 코드(+: 수평 수직 방향으로 편광된 광을 식별 가능한 측정기에 대응, ×: 경사 방향으로 편광된 광을 식별 가능한 측정기에 대응)를 랜덤으로 결정한다. 그 난수열과 송신 코드의 조합으로, 송신하는 광의 편광 방향이 자동적으로 정해진다. 여기서는, 0과 +의 조합으로 수평 방향으로 편광된 광을, 1과 +의 조합으로 수직 방향으로 편광된 광을, 0과 ×의 조합으로 45° 방향으로 편광된 광을, 1과 ×의 조합으로 135° 방향으로 편광된 광을, 양자 통신로에 각각 송신한다(송신 신호).

다음에, 수신자는, 수신 코드(+:수평 수직 방향으로 편광된 광을 식별 가능한 측정기, ×:경사 방향으로 편광된 광을 식별 가능한 측정기)를 랜덤으로 결정하고, 양자 통신로 상의 광을 측정한다(수신 신호). 그리고, 수신 코드와 수신 신호의 조합에 의해 수신 데이터를 얻는다. 여기서는, 수신 데이터로서, 수평 방향으로 편광된 광과 +의 조합으로 0을, 수직 방향으로 편광된 광과 +의 조합으로 1을, 45° 방향으로 편광된 광과 ×의 조합으로 0을, 135° 방향으로 편광된 광과 ×의 조합으로 1을, 각각 얻는다.

다음에, 수신자는, 자신의 측정이 정확한 측정기로 행해진 것인지 여부를 조사하기 위해, 수신 코드를, 공개 통신로를 거쳐 송신자에 대하여 송신한다. 수신 코드를 수취한 송신자는 정확한 측정기로 행하여진 것인지 여부를 조사하고, 그 결과를, 공개 통신로를 거쳐 수신자에 대하여 회신한다.

다음에, 수신자는, 정확한 측정기로 수신한 수신 신호에 대응하는 수신 데이터만을 남기고, 그 이외의 것을 버린다. 이 시점에서, 남겨진 수신 데이터는 송신자와 수신자 사이에서 확실히 공유되어 있다.

다음에, 송신자와 수신자는 각각의 통신 상대에 대하여 공유 데이터 중에서 선택한 소정수의 데이터를, 공개 통신로를 경유하여 송신한다. 그리고, 수취한 데이터가 자신이 가진 데이터와 일치하고 있는지 여부를 확인한다. 예컨대, 확인한 데이터 중에 일치하지 않는 데이터가 하나라도 있으면, 도청자가 있는 것으로 판단하여 공유 데이터를 버리고, 다시, 키의 공유 수순을 처음부터 한다. 한편, 확인한 데이터가 전부 일치한 경우에는, 도청자가 없다고 판단하여, 확인에 사용한 데이터를 버리고, 남은 공유 데이터를 송신자와 수신자의 공유키로 한다.

한편, 상기 종래의 양자키 배송 방법의 응용으로서, 예컨대, 전송로 상에서의 데이터 오류를 정정 가능한 양자키 배송 방법이 있다(예컨대, Brassard, G. and Salvail, L. 1993 Secret-Key Reconciliation by Public Discussion, In Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science 765, 410-423 참조).

이 방법에서는, 송신자가, 데이터 오류를 검출하기 위해, 송신 데이터를 복수의 블럭으로 분할하고, 블럭마다의 패리티를 공개 통신로 상에 송신한다. 그리고, 수신자가, 공개 통신로를 경유하여 수취한 블럭마다의 패리티와 수신 데이터에 있어서의 대응하는 블럭의 패리티를 비교하여, 데이터 오류를 체크한다. 이 때, 다른 패리티가 있었던 경우, 수신자는, 어떤 블

력의 패리티가 다른 것인지를 나타내는 정보를 공개 통신로 상에 회신한다. 그리고, 송신자는, 해당하는 블럭을 전반부의 블럭과 후반부의 블럭으로 더 분할하고, 예컨대, 전반부의 패리티를 공개 통신로 상에 회신한다(이분 탐색(二分探索)). 이후, 송신자와 수신자는 상기 이분 탐색을 반복하여 실행함으로써 오류 비트의 위치를 특정하고, 최종적으로 수신자가 그 비트를 정정한다.

또한, 송신자는, 데이터에 오류가 있음에도 불구하고, 우수개의 오류 때문에 정확하다고 판정된 패리티가 있는 경우를 상정하고, 송신 데이터를 랜덤으로 치환하여(랜덤 치환) 복수의 블럭으로 분할하고, 다시, 상기 이분 탐색에 의한 오류 정정 처리를 한다. 그리고, 랜덤 치환에 의한 이 오류 정정 처리를 반복하여 실행함으로써, 모든 데이터 오류를 정정한다.

그러나, 상기 도 10에 나타내는 종래의 양자키 배송에 있어서는, 오류 통신로를 상정하지 않기 때문에, 오류가 있는 경우에는 도청 행위가 존재한 것으로 하여 상기 공통 데이터(공통키)를 버리는 것으로 되고, 전송로에 따라서는 공통키의 생성 효율이 매우 나빠진다는 문제가 있었다.

또한, 상기 전송로 상에서의 데이터 오류를 정정 가능한 양자키 배송 방법에 있어서는, 오류 비트를 특정하기 위해 방대한 회수의 패리티의 교환이 발생하고, 또한, 랜덤 치환에 의한 오류 정정 처리가 소정 회수에 걸쳐 행하여지기 때문에, 오류 정정 처리에 막대한 시간을 쓰는 것으로 된다는 문제가 있었다.

본 발명은 상기에 감안하여 이루어진 것으로, 극히 높은 특성을 가진 오류 정정 부호를 이용하여 전송로 상에서의 데이터 오류를 정정하면서, 고도로 안전성이 보증된 공통키를 생성하는 것이 가능한 양자키 배송 방법을 제공하는 것을 목적으로 하고 있다.

발명의 상세한 설명

본 발명에 따른 양자키 배송 방법에 있어서는, 양자 통신로 상의 광자의 측정 결과로서 얻어지는 확률 정보 첨부 수신 데이터의 오류를 정정함으로써 본래의 송신 데이터를 추정하고, 그 추정 결과를 공유 정보로 하는 양자키 배송 방법으로서, 송신측 및 수신측의 통신 장치가, 개별적으로 제 1 패리티 검사 행렬(요소가 「0」 또는 「1」인 동일한 행렬)을 생성하는 제 1 검사 행렬 생성 단계와, 상기 송신측의 통신 장치가, 상기 제 1 패리티 검사 행렬과 상기 송신 데이터에 근거하여 생성한 제 1 오류 정정 정보를, 공개 통신로를 거쳐서 상기 수신측의 통신 장치에 통지하는 제 1 오류 정정 정보 통지 단계와, 상기 수신측의 통신 장치가, 상기 제 1 오류 정정 정보에 근거하여 상기 수신 데이터의 오류를 정정하는 제 1 오류 정정 단계와, 상기 수신 데이터의 오류를 완전히 정정할 수 없던 경우에, 수신측 및 송신측의 통신 장치가, 전회의 오류 정정 정보가 다음 오류 정정시의 정보의 일부가 되도록, 개별적으로 제 2 패리티 검사 행렬(요소가 「0」 또는 「1」의 동일한 행렬)을 생성하는 제 2 검사 행렬 생성 단계와, 상기 송신측의 통신 장치가, 상기 제 2 패리티 검사 행렬과 상기 송신 데이터에 근거하여 생성한 추가분의 제 2 오류 정정 정보를, 공개 통신로를 거쳐서 상기 수신측의 통신 장치에 통지하는 제 2 오류 정정 정보 통지 단계와, 상기 수신측의 통신 장치가, 상기 제 1 및 제 2 오류 정정 정보에 근거하여 상기 수신 데이터의 오류를 정정하는 제 2 오류 정정 단계와, 상기 제 1 오류 정정 단계의 처리로 수신 데이터의 오류를 완전히 정정할 수 있었던 경우, 또는, 상기 제 2 검사 행렬 생성 단계, 상기 제 2 오류 정정 정보 통지 단계, 상기 제 2 오류 정정 단계의 처리를 반복함에 의해 오류를 완전히 정정할 수 있었던 경우, 공개된 오류 정정 정보량에 따라 공유 정보의 일부를 파기하고, 그 결과를 암호키로 하는 암호키 생성 단계를 포함하는 것을 특징으로 한다.

본 발명에 의하면, 확정적인 패리티 검사 행렬을 이용하여 수신 데이터의 오류를 정정하고, 공개된 오류 정정 정보에 따라 공유 정보의 일부를 파기한다. 이에 따라, 오류 정정 처리에 걸리는 시간을 대폭 단축한다. 또한, 수신 데이터의 오류를 완전히 정정할 수 있을 때까지, 소정의 구속 조건 하에서 패리티 검사 행렬의 행수를 증가시키면서, 오류 정정 처리를 반복하여 실행한다. 이에 따라, 통신로의 잡음 레벨을 어림하기 위해 생성한 공유 정보를 파기할 필요가 없어져, 공유키의 생성 효율이 대폭 향상한다.

도면의 간단한 설명

도 1은 본 발명에 따른 양자 암호 시스템의 구성을 나타내는 도면,

도 2는 본 발명에 따른 양자키 배송의 처리를 나타내는 흐름도,

도 3은 유한 아핀 기하에 근거한 「Irregular-LDPC 부호」의 구성법을 나타내는 흐름도,

도 4는 유한 아핀 기하 부호 AG(2, 2^2)의 매트릭스를 나타내는 도면,

도 5는 최종적인 열의 가중치 배분과 행의 가중치 배분을 나타내는 도면,

도 6은 송신측의 통신 장치가 수신측의 통신 장치에 대하여 송신하는 신드롬을 도시하는 도면,

도 7은 본 실시예의 패리티 검사 행렬 생성 방법을 도시하는 도면,

도 8은 단계 S15의 처리에 의해서 경(硬) 판정값 m_B의 오류를 완전히 정정할 수 있었던 경우의, 실시예 2의 동작을 도시하는 도면,

도 9는 단계 S15의 처리에 의해서 경 판정값 m_B의 오류를 완전히 정정할 수 있었던 경우의, 실시예 3의 동작을 도시하는 도면,

도 10은 종래의 양자키 배송의 개요를 나타내는 도면이다.

실시예

이하에, 본 발명에 따른 양자키 배송 방법 및 통신 장치의 실시예를 도면에 근거하여 상세히 설명한다. 또, 이 실시예에 의해 본 발명이 한정되는 것이 아니다. 또한, 이하에서는, 예로서 편광을 이용하는 양자키 배송에 대하여 설명하지만, 본 발명은, 예컨대, 위상을 이용하는 것, 주파수를 이용하는 것 등에도 적용 가능하고, 어떠한 양자 상태를 이용하는지에 대해서는 특히 한정하지 않는다.

(실시예 1)

양자키 배송은, 도청자의 계산 능력에 상관없이, 안전성이 보증된 키 배송 방식이지만, 예컨대, 보다 효율적으로 공유키를 생성하기 위해서는, 전송로를 지나는 것에 따라 발생하는 데이터의 오류를 제거할 필요가 있다. 그래서, 본 실시예에서는, 극히 높은 특성을 갖는 것이 알려져 있는 저밀도 패리티 검사(LDPC: Low-Density Parity-Check) 부호를 이용하여 오류 정정을 하는 양자키 배송에 대하여 설명한다.

도 1은 본 발명에 따른 양자 암호 시스템(송신측 및 수신측의 통신 장치)의 구성을 나타내는 도면이다. 이 양자 암호 시스템은, 정보 m_a를 송신하는 기능을 구비한 송신측의 통신 장치와, 전송로 상에서 잡음 등의 영향을 받은 정보 m_a, 즉 정보 m_b를 수신하는 기능을 구비한 수신측의 통신 장치로 구성된다.

또한, 송신측의 통신 장치는, 양자 통신로를 거쳐서 정보 m_a를 송신하고, 공개 통신로를 거쳐서 신드롬 S_A를 송신하며, 이들 송신 정보에 근거하여 암호키(수신측과의 공통키)를 생성하는 암호키 생성부(1)와, 암호화부(21)가 암호키에 근거하여 암호화한 데이터를, 송수신부(22)가 공개 통신로를 거쳐 주고받는 통신부(2)를 구비하고, 수신측의 통신 장치는, 양자 통신로를 거쳐서 정보 m_b를 수신하며, 공개 통신로를 거쳐서 신드롬 S_A를 수신하고, 이들 수신 정보에 근거하여 암호키(송신측과의 공통키)를 생성하는 암호키 생성부(3)와, 암호화부(42)가 암호키에 근거하여 암호화한 데이터를, 송수신부(41)가 공개 통신로를 거쳐 교환하는 통신부(4)를 구비한다.

상기 송신측의 통신 장치에서는, 양자 통신로 상에 송신하는 정보 m_a로서, 편광 필터를 이용하여 소정의 방향으로 편광시킨 광(도 10 참조)을, 수신측의 통신 장치에 대하여 송신한다. 한편, 수신측의 통신 장치에서는, 수평 수직 방향(0°, 90°)의 편광을 식별 가능한 측정기와 경사 방향(45°, 135°)의 편광을 식별 가능한 측정기를 이용하여, 양자 통신로 상의, 수평 방향(0°)으로 편광된 광과 수직 방향(90°)으로 편광된 광과 45° 방향으로 편광된 광과 135° 방향으로 편광된 광을 식별한다. 또, 각 측정기는, 규정된 방향으로 편광된 광에 대해서는 정확하게 인식할 수 있지만, 예컨대, 경사 방향으로 편광된 광을 수평 수직 방향(0°, 90°)의 편광을 식별 가능한 측정기에 의해 측정하면, 수평 방향과 수직 방향으로 편광된 광을 각각 50%의 확률로 랜덤으로 식별한다. 즉, 식별 가능한 편광 방향에 대응하지 않는 측정기를 이용한 경우에는, 그 측정 결과를 해석하더라도, 편광된 방향을 정확하게 식별할 수가 없다.

이하, 상기 양자 암호 시스템에서의 각 통신 장치의 동작, 즉, 본 실시예에서의 양자키 배송에 대하여 상세히 설명한다. 도 2는 본 실시예의 양자키 배송을 나타내는 흐름도, 상세하게는, (a)는 송신측의 통신 장치의 처리를 나타내고, (b)는 수신측의 통신 장치의 처리를 나타낸다.

우선, 상기 송신측의 통신 장치 및 수신측의 통신 장치에서는, 패리티 검사 행렬 생성부(10, 30)가, 특정 선형 부호의 패리티 검사 행렬 H(n×k의 행렬)을 구하며, 이 패리티 검사 행렬 H로부터 「HG=0」을 만족시키는 생성 행렬 G((n-k)×n의 행렬)을 구하고, 또한, G^{-1}·G=I(단위 행렬)로 되는 G의 역행열 G^{-1}(n×(n-k)의 행렬)을 구한다(단계 S1, 단계 S11). 본 실시예에서는, 상기 특정 선형 부호로서, 샤논한계(Shannon limit)에 극히 가까운 우수한 특성을 갖는 LDPC 부호를 이용한 경우의 양자키 배송에 대하여 설명한다. 또, 본 실시예에서는, 오류 정정 방식으로서 LDPC 부호를 이용하는 것으로 했지만, 이것에 한정되지 않고, 예컨대, 터보 부호 등의 다른 선형 부호를 이용하는 것으로 해도 좋다. 또한, 예컨대, 후술하는 오류 정정 정보(신드롬)가 적당한 행렬 H와 송신 데이터 m_A(정보 m_a의 일부)의 적 Hm_A로 표시되는 오류 정정 프로토콜(예컨대, 종래 기술에서 설명한 「전송로 상에서의 데이터 오류를 정정 가능한 양자키 배송」에 상당하는 오류 정정 프로토콜)이면, 즉, 오류 정정 정보와 송신 데이터 m_A의 선형성이 확보되는 것이면, 그 행렬 H를 이용하는 것으로 해도 좋다.

여기서, 상기 패리티 검사 행렬 생성부(10)에서의 LDPC 부호용 검사 행렬의 구성법에 대하여 설명한다. 본 실시예에서는, 일례로서, 유한 아핀 기하에 근거한 「Irregular-LDPC 부호」용 검사 행렬의 구성법(도 2 단계 S1의 상세)에 대하여 설명한다. 도 3은 유한 아핀 기하에 근거한 「Irregular-LDPC 부호」용 검사 행렬의 구성법을 나타내는 흐름도이다. 또, 패리티 검사 행렬 생성부(30)에 대해서는, 패리티 검사 행렬 생성부(10)와 마찬가지로 동작하기 때문에 그 설명을 생략한다. 또한, 본 실시예에서의 패리티 검사 행렬 생성 처리는, 예컨대, 설정되는 파라미터에 따라 패리티 검사 행렬 생성부(10)로 실행하는 구성으로 해도 좋고, 통신 장치 외부의 다른 제어 장치(계산기 등)로 실행하는 것으로 해도 좋다. 본 실시예에서의 패리티 검사 행렬 생성 처리가 통신 장치 외부에서 실행되는 경우는, 생성 완료된 패리티 검사 행렬이 통신 장치에 저장된다. 이후의 실시예에서는, 패리티 검사 행렬 생성부(10)에서 상기 처리를 실행하는 경우에 대하여 설명한다.

우선, 패리티 검사 행렬 생성부(10)에서는, 「Irregular-LDPC 부호」용의 검사 행렬의 베이스로 되는 유한 아핀 기하 부호 AG(2, 2^s)를 선택한다(도 3, 단계 S21). 여기서는, 행의 가중치와 열의 가중치가 각각 2^s로 된다. 도 4는, 예컨대, 유한 아핀 기하 부호 AG(2, 2^2)의 매트릭스를 도시한 도면(공백은 0을 나타낸다)이다.

다음에, 패리티 검사 행렬 생성부(10)에서는, 열의 가중치의 최대값 r_1($2<r_1\leq 2^s$)을 결정한다(단계 S22). 그리고, 부호화율 레이트(1 신드롬 길이/키의 길이)를 결정한다(단계 S22).

다음에, 패리티 검사 행렬 생성부(10)에서는, 가우스 근사법(Gaussian Approximation)에 의한 최적화를 이용하여, 잠정적으로, 열의 가중치 배분 $\lambda(\gamma_i)$와 행의 가중치 배분 ρ_u를 구한다(단계 S23). 또, 행의 가중치 배분의 생성함수 $\rho(x)$는 $\rho(x)=\rho_u x^{u-1}+(1-\rho_u)x^u$로 한다. 또한, 가중치 u는 u≥2의 정수이며, ρ_u는 행에서의 가중치 u의 비율을 나타낸다.

다음에, 패리티 검사 행렬 생성부(10)에서는, 유한 아핀 기하의 행의 분할에 의해 구성 가능한, 행의 가중치 {u, u+1}을 선택하고, 또한 (1)식을 만족시키는 분할 계수 $\{b_u, b_{u+1}\}$을 구한다(단계 S24). 또, b_u, b_{u+1}은 비부(非負)의 정수로 한다.

$$b_u+b_{u+1}(u+1)=2^s \quad \cdots (1)$$

구체적으로는, 하기 (2)식으로부터 b_u를 구하고, 상기 (1)식으로부터 b_{u+1}을 구한다.

$$\arg\min_{bu}\left|\varphi_u-\frac{u\times b_u}{2^s}\right| \quad \cdots (2)$$

다음에, 패리티 검사 행렬 생성부(10)에서는, 상기 결정한 파라미터 u, u+1, b_u, b_{u+1}에 의해 갱신된 행의 가중치의 비율 ρ_u', ρ_{u+1}'을 (3)식에 의해 구한다(단계 S25).

$$\varphi_u' = \frac{u \times b_u}{2^s}$$
$$\varphi_{u+1}' = \frac{(u+1) \times b_{u+1}}{2^s} \quad \cdots (3)$$

다음에, 패리티 검사 행렬 생성부(10)에서는, 가우스 근사법에 의한 최적화를 이용하고, 또한 상기에서 구한 u, u+ 1, ρ_u', ρ_{u+1}'을 고정 파라미터로 하여, 잠정적으로 열의 가중치 배분 $\lambda(\gamma_i)$을 구한다(단계 S26). 또, 가중치 γ_i는 $\gamma_i \geq 2$의 정수이며, $\lambda(\gamma_i)$는 열에서의 가중치 γ_i의 비율을 나타낸다. 또한, 열수가 1 이하로 되는 가중치($\lambda(\gamma_i) \leq \gamma_i/w_t$, i는 정의 정수)를 후보에서 삭제한다. 단, w_t는 AG(2, 2^s)에 포함되는 1의 총수를 나타낸다.

다음에, 상기에서 구한 가중치 배분을 만족시키고, 또한 하기 (4)식을 만족시키는 열의 가중치 후보의 세트 {γ_1, γ_2, $\cdots\gamma_l$($\gamma_l \leq 2^s$)}를 선택한다(단계 S27). 그리고, 하기의 (4)식을 만족시키지 않는 열의 가중치 γ_i가 존재하는 경우에는, 그 열의 가중치를 후보로부터 삭제한다.

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,\ell} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,\ell} \\ \vdots & & \cdots & \vdots \end{bmatrix} \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_\ell \end{bmatrix} = \begin{bmatrix} 2^s \\ 2^s \\ \vdots \\ 2^s \end{bmatrix} \quad \cdots (4)$$

또, 각 a는, 열의 가중치 2^s를 구성하기 위한 {γ_1, γ_2, $\cdots\gamma_l$}에 대한 비부의 정수로 되는 계수를 나타내고, i, j는 정의 정수이며, γ_l는 열의 가중치를 나타내고, γ_l은 열의 최대가중치를 나타낸다.

다음에, 패리티 검사 행렬 생성부(10)에서는, 가우스 근사법에 의한 최적화를 이용하고, 또한 상기에서 구한 u, u+ 1, ρ_u', ρ_{u+1}'과 {γ_1, γ_2, $\cdots\gamma_l$}을 고정 파라미터로 하여, 열의 가중치 배분 $\lambda(\gamma_i)$과 행의 가중치 배분 ρ_u를 구한다(단계 S28).

다음에, 패리티 검사 행렬 생성부(10)에서는, 분할 처리를 하기 전에, 열의 가중치 배분 $\lambda(\gamma_i)$와 행의 가중치 배분 ρ_u를 조정한다(단계 S29). 또, 조정후의 각 가중치의 배분은, 가능한 한 가우스 근사법으로 구한 값에 가까운 값으로 한다. 도 5는 단계 S29에 있어서의 최종적인 열의 가중치 배분 $\lambda(\gamma_i)$와 행의 가중치 배분 ρ_u를 나타내는 도면이다. 또한 $n(\gamma_i)$은 가중치 단위의 총열수를 나타내고, n_u는 가중치 단위의 총행수를 나타낸다.

마지막으로, 패리티 검사 행렬 생성부(10)에서는, 상기 처리에서 구한 각 가중치 배분에 근거하여, 유한 아핀 기하에 있어서의 행 및 열을 분할하여(단계 S30), n×k의 패리티 검사 행렬 H를 생성한다. 본 발명에서의 유한 아핀 기하 부호의 분할 처리는, 각 행 또는 각 열에서 「1」을 랜덤으로 추출하고, 불규칙적으로 분할(랜덤 분할)한다. 또, 이 추출 처리는, 랜덤성이 유지되는 것이면 어떠한 방법을 이용하여도 좋다.

이와 같이, 본 실시예에서는, 예컨대, 상기 유한 아핀기하에 근거한 「Irregular-LDPC 부호」용 검사 행렬의 구성법(도 2, 단계 S1)을 실행함으로써, 확정적이고 특성이 안정한 「Irregular-LDPC 부호」용의 검사 행렬 H(n×k)을 생성했다. 또, 본 실시예에 있어서는, 기본으로 되는 부호(기본행렬)에 유한 아핀기하를 이용하는 것으로 했지만(단계 S21), 이것에 한정되지 않고, 「행과 열의 가중치가 일정하다」 또한 「2부 그래프상의 사이클수가 6 이상」이라는 조건을 만족시키는 행렬이면, 유한 아핀기하 이외(케일리 그래프에 의한 기본행렬이나 라마누잔 그래프에 의한 기본행렬 등)의 행렬을 이용하는 것으로 해도 좋다. 또한, 본 실시예에서는, 일례로서, 상기 단계 S21~S29를 이용하여 유한 아핀기하에 근거한 「Irregular-LDPC 부호」용 검사 행렬을 생성했지만, 상기 단계 S1 및 S11에서 생성하는 검사 행렬 H에 대해서는 이것에 한정되지 않고, 상기 이외의 구성법으로 생성하는 것으로 해도 좋다.

상기한 바와 같이, 패리티 검사 행렬 H를 생성하고, 그 후, 생성 행렬 G, G^{-1}($G^{-1} \cdot G = I$:단위행렬)을 생성 후, 다음에, 송신측의 통신 장치에서는, 난수 발생부(11)가, 난수열인 정보 m_a(1,0의 열: 송신 데이터)를 발생하고, 또한 송신 코드(+ :수평 수식 방향으로 편광된 광을 식별 가능한 측정기에 대응한 코드, ×:경사 방향으로 편광된 광을 식별 가능한 측정기에 대응한

코드)를 랜덤으로 결정한다(단계 S2). 한편, 수신측의 장치에서는, 난수 발생부(31)가, 수신 코드(+ :수평 수직 방향으로 편광된 광을 식별 가능한 측정기에 대응한 코드, ×:경사 방향으로 편광된 광을 식별 가능한 측정기에 대응한 코드)를 랜덤으로 결정한다(단계 S12).

다음에, 송신측의 통신 장치에서는, 광자 생성부(12)가, 상기 정보 m_a와 송신 코드의 조합으로 자동적으로 결정되는 편광 방향에서 광자를 송신한다(단계 S3). 예컨대, 0과 + 의 조합으로 수평 방향으로 편광된 광을, 1과 + 의 조합으로 수직 방향으로 편광된 광을, 0과 ×의 조합으로 45° 방향으로 편광된 광을, 1과 ×의 조합으로 135° 방향으로 편광된 광을, 양자 통신로에 각각 송신한다(송신 신호).

광자 생성부(12)의 광 신호를 수취한 수신측의 통신 장치의 광자 수신부(32)에서는, 양자 통신로 상의 광을 측정한다(수신 신호). 그리고, 수신 코드와 수신 신호의 조합에 의해 자동적으로 결정되는 정보 m_b(1, 0의 열: 수신 데이터)를 얻는다(단계 S13). 여기서는, 수신 데이터 m_b로서, 수평 방향으로 편광된 광과 + 의 조합으로 0을, 수직 방향으로 편광된 광과 + 의 조합으로 1을, 45° 방향으로 편광된 광과 ×의 조합으로 0을, 135° 방향으로 편광된 광과 ×의 조합으로 0을, 각각 얻는다. 또, 수신 데이터 m_b는 확률 정보 첨부의 경 판정값으로 한다.

다음에, 수신측의 통신 장치에서는, 상기 측정이 정확한 측정기로 행하여진 것인지 여부를 조사하기 위해, 난수 발생부(31)가, 수신 코드를, 공개 통신로 통신부(34), 공개 통신로를 거쳐 송신측의 통신 장치에 대하여 송신한다(단계 S13). 수신 코드를 수취한 송신측의 통신 장치에서는, 난수 발생부(11)가, 상기 측정이 정확한 측정기로 행하여진 것인지 여부를 조사하고, 그 결과를, 공개 통신로 통신부(13), 공개 통신로를 거쳐 수신측의 통신 장치에 대하여 송신한다(단계 S3). 그리고, 수신측의 통신 장치 및 송신측의 통신 장치에서는, 정확한 측정기로 수신한 수신 신호에 대응하는 데이터만을 남기고, 그 나머지를 버린다(단계 S3, S13). 그 후, 남은 데이터를 메모리 등에 저장하고, 그 선두로부터 순서대로 n 비트를 판독하고, 이것을, 정식인 송신 데이터 m_A와 수신 데이터 m_B(m_B는 전송로 상에서 잡음 등의 영향을 받은 m_A:$m_B=m_A+e$(잡음 등))로 한다. 이에 따라, 남은 데이터의 비트 위치를, 송신측의 통신 장치와 수신측의 통신 장치 사이에서 공유할 수 있다. 또, 수신 데이터 m_B는, 상기 m_B와 마찬가지로, 확률 정보 첨부의 경 판정값이다.

다음에, 송신측의 통신 장치에서는, 신드롬 생성부(14)가, 패리티 검사 행렬 H(n×k의 행렬)와 송신 데이터 m_A을 이용하여 m_A의 신드롬 $S_A=Hm_A$를 계산하고, 그 결과를, 공개 통신로 통신부(13), 공개 통신로를 거쳐 수신측의 통신 장치에 통지한다(단계 S4). 이 단계에서, m_A의 신드롬 S_A(k 비트분의 정보)는 도청자에게 알려질 가능성이 있다. 도 6은 송신측의 통신 장치가 수신측의 통신 장치에 대하여 송신하는 신드롬을 도시하는 도면이다. 한편, 수신측의 통신 장치에서는, 공개 통신로 통신부(34)에서 m_A의 신드롬 S_A를 수신하고, 그것을 신드롬 복호부(33)에 통지한다(단계 S14).

다음에, 신드롬 복호부(33)에서는, 기지의 신드롬 복호법을 이용하여, 잡음 등에 의한 확률 정보 첨부의 경 판정값 m_B의 오류를 정정함으로써 본래의 송신 데이터 m_A를 추정한다(단계 S15). 본 실시예에서는, 예컨대, 「$S_A=Hm_C$」을 만족시키는 m_C를 확률 정보 첨부의 경 판정값 m_B로부터 추정하고, 그 추정 결과 m_C를 공유 정보 m_A로 한다. 또, 본 실시예에 있어서는, 수신 데이터 m_B 및 m_b를 확률 정보 첨부의 경 판정값으로 했지만, 이것에 한정되지 않고, 예컨대, 연(軟) 판정값으로 한 경우에도 적용 가능하고, 어떠한 수신 데이터를 이용할지에 대해서는 특히 규정하지 않는다.

그리고, 단계 S15의 처리에 의해 경 판정값 m_B의 오류를 완전히 정정할 수 있었던 경우(단계 S15, 예), 수신측의 통신 장치에서는, 공유키 생성부(35)가, 공개된 오류 정정 정보(도청되었을 가능성이 있는 상기 k 비트분의 정보: S_A)에 따라 공유 정보 m_A의 일부를 버려, n-k 비트분의 정보량을 구비한 암호키 r을 생성한다(단계 S16). 즉, 공유키 생성부(35)에서는, 먼저 계산해 놓은 G^{-1}(n×(n-k)의 행렬)을 이용하여 하기 (5)식에 의해 암호키 r을 생성한다. 수신측의 통신 장치는, 이 암호키 r을 송신측의 통신 장치와의 공유키로 한다.

$$r = G^{-1}m_A \qquad \cdots (5)$$

또한, 송신측의 통신 장치에 있어서는, 단계 S15의 처리에 의해서 경 판정값 m_B의 오류가 완전히 정정되고, 새로운 신드롬 요구가 없는 경우(단계 S5, 예), 공유키 생성부(15)가, 공개된 오류 정정 정보(도청되었을 가능성이 있는 상기 k 비트분의

정보: S_A)에 따라 공유 정보 m_A의 일부를 버려, n-k 비트분의 정보량을 갖춘 암호키 r을 생성한다(단계 S6). 즉, 공유키 생성부(15)에서도, 먼저 계산해 놓은 G^{-1}(n×(n-k)의 행렬)을 이용하여 상기 (5)식에 의해 암호키 r을 생성한다(단계 S6). 송신측의 통신 장치는, 이 암호키 r을 수신측의 통신 장치와의 공유키로 한다.

또, 본 실시예에 있어서는, 또한, 정칙인 랜덤 행렬 R을 이용하여 상기 공유키를 정렬하는 구성으로 해도 좋다. 이에 따라, 비닉성을 증강시킬 수 있다. 구체적으로는, 우선, 송신측의 통신 장치가, 정칙인 랜덤 행렬 R((n-k)×(n-k)의 행렬)을 생성하고, 또한, 당해 R을, 공개 통신로를 거쳐 수신측의 통신 장치에 통지한다. 또, 이 처리는, 수신측의 통신 장치에서 실행하는 것으로 해도 좋다. 그 후, 송신측 및 수신측의 통신 장치가, 먼저 계산해 놓은 G^{-1}(n×(n-k)의 행렬)과 랜덤 행렬 R을 이용하여 하기 (6)식에 의해 암호키 r을 생성한다.

$$r = RG^{-1}m_A \qquad \cdots (6)$$

한편, 단계 S15의 처리에 의해 경 판정값 m_B의 오류를 완전히 정정할 수 없던 경우(단계 S15, 아니오), 수신측의 통신 장치의 신드롬 복호부(33)에서는, 공개 통신로 통신부(34), 공개 통신로를 거쳐 송신측의 통신 장치에 신드롬 요구를 통지한다(단계 S17). 그리고, 패리티 검사 행렬 생성부(30)에서는, 상기 도 3에 나타내는 방법 또는 그것과는 다른 기지의 방법에 의해 패리티 검사 행렬 H'(n×(k+t)의 행렬)을 생성하고, 그 후, 이 패리티 검사 행렬 H'로부터 「H'G'=0」를 만족시키는 생성 행렬 G', G'^{-1}(G'^{-1}·G'=I:단위행렬)을 생성한다(단계 S18). 이 경우, 패리티 검사 행렬 H'은, 「상기 단계 S4에서 생성한 신드롬 S_A를 유지한다」라는 구속 조건 하에서 생성한다. 도 7은 본 실시예의 패리티 검사 행렬 생성 방법을 도시하는 도면이다. 또, t의 사이즈는 시스템의 요구 조건에 의존한다. 예컨대, t의 사이즈를 작게 한 경우에는, 오류 정정 처리의 회수를 증가시켜 버릴 가능성이 있지만, 한편으로, 키의 생성율이 향상한다. 또한, t의 사이즈를 크게 한 경우에는, 오류 정정 처리의 회수를 저감할 수 있지만, 한편으로, 키의 생성율이 저하한다.

다음에, 신드롬 요구를 수취한(단계 S5, 아니오) 송신측의 통신 장치의 패리티 검사 행렬 생성부(10)에 있어서도, 상기 도 3에 나타내는 방법 또는 그것과는 다른 기지의 방법에 의해 패리티 검사 행렬 H'(n×(k+t)의 행렬)을 생성하고, 그 후, 이 패리티 검사 행렬 H'로부터 「H'G'=0」를 만족시키는 생성 행렬 G', G'^{-1}(G'^{-1}·G'=I:단위행렬)을 생성한다(단계 S7). 이 경우의 패리티 검사 행렬 H'도, 상기와 같이 「상기 단계 S4에서 생성한 신드롬을 유지한다」라는 구속 조건 하에서 생성한다.

다음에, 송신측의 통신 장치에서는, 신드롬 생성부(14)가, 패리티 검사 행렬 H'(n×(k+t)의 행렬)과 송신 데이터 m_A를 이용하여 도 7에 나타내는 t 행분의 신드롬 S_A'를 계산하고, 그 결과를, 공개 통신로 통신부(13), 공개 통신로를 거쳐 수신측의 통신 장치에 통지한다(단계 S8). 또, 이 단계에서, 신드롬 S_A'(t 비트분의 정보)는 도청자에게 알려질 가능성이 있다. 그리고, 수신측의 통신 장치에서는, 공개 통신로 통신부(34)에서 t 행분의 신드롬 S_A'를 수신하고, 그것을 신드롬 복호부(33)에 통지한다(단계 S19).

다음에, 신드롬 복호부(33)에서는, 상기 기지의 신드롬 복호법을 이용하여, 확률 정보 첨부의 경 판정값 m_B의 오류를 정정하고, 다시, 본래의 송신 데이터 m_A를 추정한다(단계 S15).

이후, 본 실시예의 수신측의 통신 장치에 있어서는, 단계 S15의 처리에 의해 경 판정값 m_B의 오류를 완전히 정정할 수 있을 때까지, 패리티 검사 행렬의 행수를 증가시키면서 단계 S17~S19의 처리를 반복하여 실행하고, 오류를 완전히 정정할 수 있었던 단계에서, 공유키 생성부(35)가, 공개된 오류 정정 정보(예컨대, 도청되었을 가능성이 있는 상기 k+t 비트분의 정보: S_A+S_A'(도 7 참조))에 따라 공유 정보 m_A의 일부를 버려, 예컨대, n-k-t, n-k-2t, n-k-3t, … 비트분의 정보량을 갖춘 암호키 r을 생성한다(단계 S16). 수신측의 통신 장치는, 이 암호키 r을 송신측의 통신 장치와의 공유키로 한다.

또한, 본 실시예의 송신측의 통신 장치에 있어서는, 새로운 신드롬 요구가 통지되지 않을 때까지, 패리티 검사 행렬의 행수를 증가시키면서 단계 S7, S8의 처리를 반복하여 실행하고, 새로운 신드롬 요구가 통지되지 않은 단계에서, 공유키 생성부(15)가, 공개된 오류 정정 정보(예컨대, 도청되었을 가능성이 있는 상기 k+t 비트분의 정보:S_A+S_A'(도 7 참조))에 따라 공유 정보 m_A의 일부를 버려, 예컨대, n-k-t, n-k-2t, n-k-3t, … 비트분의 정보량을 갖춘 암호키 r을 생성한다(단계 S6). 송신측의 통신 장치는, 이 암호키 r을 수신측의 통신 장치와의 공유키로 한다.

이와 같이, 본 실시예에서는, 확정적이고 특성이 안정한 「Irregular-LDPC 부호」 용의 검사 행렬을 이용하여 수신 데이터의 오류를 정정하고, 공개된 오류 정정 정보에 따라 공유 정보의 일부를 버리는 구성으로 했다. 이에 따라, 오류 비트를 특정/정정하기 위한 방대한 회수의 패리티의 교환이 없어져, 오류 정정 정보를 송신하는 것만으로 오류 정정 제어가 행하여지기 때문에, 오류 정정 처리에 걸리는 시간을 대폭 단축시킬 수 있다. 또한, 공개된 정보에 따라 공유 정보의 일부를 버리고 있기 때문에, 고도로 안전성이 보증된 공통키를 생성할 수 있다.

또한, 본 실시예에서는, 수신 데이터의 오류를 완전히 정정할 수 있을 때까지, 소정의 구속 조건 하에서 패리티 검사 행렬의 행수를 증가시키면서, 오류 정정 처리를 반복하여 실행하는 구성으로 했다. 이에 따라, 통신로의 잡음 레벨을 어림하기 위해 생성한 공유 정보를 파기할 필요가 없어지기 때문에, 공유키의 생성 효율을 대폭 향상시킬 수 있다.

(실시예 2)

이어서, 실시예 2의 양자키 배송 방법에 대하여 설명한다. 또, 송신측의 통신 장치 및 수신측의 통신 장치의 구성에 대해서는, 먼저 설명한 실시예 1의 구성과 마찬가지기 때문에, 동일한 부호를 부여하여 그 설명을 생략한다.

도 8은, 상기 단계 S15의 처리에 의해서 경 판정값 m_B의 오류를 완전히 정정할 수 있었던 경우의, 실시예 2의 동작을 도시하는 도면이다. 여기서는, 도 2를 이용하여, 본 실시예의 특징적인 동작인 단계 S17~S19, S7, S8의 처리에 대하여 설명한다.

예컨대, 단계 S15의 처리에 의해서 경 판정값 m_B의 오류를 완전히 정정할 수 없던 경우(단계 S15, 아니오), 그 오류를 완전히 정정하기 위해, 수신측의 통신 장치의 신드롬 복호부(33)에서는, 공개 통신로 통신부(34), 공개 통신로를 거쳐 송신측의 통신 장치에 신드롬 요구를 통지한다(단계 S17).

그리고, 패리티 검사 행렬 생성부(30)에서는, 패리티 검사 행렬 H를 유지한 상태로, 도 8에 도시하는 바와 같이 t행분의 행렬 H''(n×t의 행렬)을 추가 생성하고, 그 후, 본래의 패리티 검사 행렬 H와 행렬 H''을 조합한 행렬 H'(n×(k+t)의 행렬)로부터 「H'G'=0」를 만족시키는 생성 행렬 G', G-1'(G-1'·G'=I:단위행렬)을 생성한다(단계 S18). 이 경우, 행렬 H''의 가중치 배분은, 「패리티 검사 행렬 H'이 rankH'=k+t로 되는 것(선형 독립인 것)」, 「패리티 검사 행렬 H'이 본래의 패리티 검사 행렬 H를 유지하는 것」과 같은 구속 조건 하에서, 상기 도 3에 나타내는 방법 또는 그것과는 다른 기지의 방법에 의해 생성한다. 또, t의 사이즈는, 시스템의 요구 조건에 의존한다. 예컨대, t의 사이즈를 작게 한 경우에는, 오류 정정 처리의 회수를 증가시켜 버릴 가능성이 있지만, 한편으로, 키의 생성율이 향상한다. 또한, t의 사이즈를 크게 한 경우에는, 오류 정정 처리의 회수를 저감할 수 있지만, 한편으로, 키의 생성율이 저하한다.

또한, 신드롬 요구를 수취한(단계 S5, 아니오) 송신측의 통신 장치의 패리티 검사 행렬 생성부(10)에 있어서도, 상기와 동일한 처리로, 패리티 검사 행렬 H를 유지한 상태로 t 행분의 행렬 H''를 추가 생성하고(도 8 참조), 그 후, 본래의 패리티 검사 행렬 H와 행렬 H''을 조합한 행렬 H'로부터 「H'G'=0」를 만족시키는 생성 행렬 G', G^{-1}'(G^{-1}'·G'=I:단위행렬)을 생성한다(단계 S7).

다음에, 송신측의 통신 장치에서는, 신드롬 생성부(14)가, 패리티 검사 행렬 H'과 송신 데이터 m_A을 이용하여 도 8에 나타내는 t 행분의 신드롬 S_A'를 계산하고, 그 결과를, 공개 통신로 통신부(13), 공개 통신로를 거쳐 수신측의 통신 장치에 통지한다(단계 S8). 또, 이 단계에서, 신드롬 S_A'(t 비트분의 정보)는 도청자에게 알려질 가능성이 있다. 그리고, 수신측의 통신 장치에서는, 공개 통신로 통신부(34)에 의해 t 행분의 신드롬 S_A'를 수신하고, 그것을 신드롬 복호부(33)에 통지한다(단계 S19).

다음에, 신드롬 복호부(33)에서는, 기지의 신드롬 복호법을 이용하여, 확률 정보 첨부의 경 판정값 m_B의 오류를 정정하고, 다시, 본래의 송신 데이터 m_A를 추정한다(단계 S15). 본 실시예에서는, 예컨대, 「$(S_A+S_A')=H'm_C$」을 만족시키는 m_C를 확률 정보 첨부의 경 판정값 m_B로부터 추정하고, 그 추정 결과 m_C를 공유 정보 m_A로 한다.

이후, 본 실시예의 수신측의 통신 장치에 있어서는, 단계 S15의 처리에 의해 경 판정값 m_B의 오류를 완전히 정정할 수 있을 때까지, 패리티 검사 행렬의 행수를 증가시키면서 단계 S17~S19의 처리를 반복하여 실행하고, 오류를 완전히 정정할

수 있었던 단계에서, 공유키 생성부(35)가, 공개된 오류 정정 정보(예컨대, 도청되었을 가능성이 있는 상기 k+t 비트분의 정보: S_A+S_A'(도 8 참조))에 따라 공유 정보 m_A의 일부를 버리고, 예컨대, n-k-t, n-k-2t, n-k-3t, … 비트분의 정보량을 갖춘 암호키 r을 생성한다(단계 S16). 수신측의 통신 장치는, 이 암호키 r을 송신측의 통신 장치와의 공유키로 한다.

또한, 본 실시예의 송신측의 통신 장치에 있어서는, 새로운 신드롬 요구가 통지되지 않을 때까지, 패리티 검사 행렬의 행수를 증가시키면서 단계 S7, S8의 처리를 반복하여 실행하고, 새로운 신드롬 요구가 통지되지 않은 단계에서, 공유키 생성부(15)가, 공개된 오류 정정 정보(예컨대, 도청되었을 가능성이 있는 상기 k+t 비트분의 정보: S_A+S_A'(도 8 참조))에 따라 공유 정보 m_A의 일부를 버리고, 예컨대, n-k-t, n-k-2t, n-k-3t, … 비트분의 정보량을 갖춘 암호키 r을 생성한다(단계 S6). 송신측의 통신 장치는, 이 암호키 r을 수신측의 통신 장치와의 공유키로 한다.

이와 같이, 본 실시예에서는, 실시예 1와 마찬가지로, 수신 데이터의 오류를 완전히 정정할 수 있을 때까지, 소정의 구속 조건 하에서 패리티 검사 행렬의 행수를 증가시키면서, 오류 정정 처리를 반복하여 실행하는 구성으로 했다. 이에 따라, 통신로의 잡음 레벨을 어림하기 위해 생성한 공유 정보를 파기할 필요가 없어지기 때문에, 공유키의 생성 효율을 대폭 향상시킬 수 있다.

(실시예 3)

계속해서, 실시예 3의 양자키 배송 방법에 대하여 설명한다. 실시예 1 및 2에서는, 공개된 오류 정정 정보에 따라 공유 정보 m_A의 일부를 버려 암호키 r을 생성하고 있었다. 즉, 오류 정정 처리를 반복할 때마다, 암호키 r의 키 길이가 줄어들고 있었다. 이것에 비하여, 본 실시예에서는, 하기의 처리에 의해서 항상 일정 길이의 암호키 r을 생성한다. 또, 송신측의 통신 장치 및 수신측의 통신 장치의 구성에 대해서는, 먼저 설명한 실시예 1의 구성과 마찬가지기 때문에, 동일한 부호를 부여하여 그 설명을 생략한다.

도 9는, 상기 단계 S15의 처리에 의해서 경 판정값 m_B의 오류를 완전히 정정할 수 없던 경우의, 실시예 3의 동작을 도시하는 도면이다. 여기서는, 도 2를 이용하여, 본 실시예의 특징적인 동작인 단계 S17~S19, S7, S8의 처리에 대하여 설명한다.

예컨대, 단계 S15의 처리에 의해서 경 판정값 m_B의 오류를 완전히 정정할 수 없던 경우(단계 S15, 아니오), 그 오류를 완전히 정정하기 위해, 수신측의 통신 장치의 신드롬 복호부(33)에서는, 공개 통신로 통신부(34), 공개 통신로를 거쳐 송신측의 통신 장치에 신드롬 요구를 통지한다(단계 S17).

그리고, 패리티 검사 행렬 생성부(30)에서는, 패리티 검사 행렬 H를 유지한 상태로, 도 9에 도시하는 바와 같이 t 행분의 행렬 H'''((n+t)×t의 행렬)을 추가 생성하고, 그 후, 본래의 패리티 검사 행렬 H와 t 열분의 0행렬(t×k의 0행렬)과 상기 행렬 H'''을 조합한 행렬 H'((n+t)×(k+t)의 행렬)로부터, 「H'G'=0」를 만족시키는 생성 행렬 G', G^{-1}(G^{-1}·G'=I:단위행렬)을 생성한다(단계 S18). 이 경우, 행렬 H'''의 각 성분은, 「패리티 검사 행렬 H'이 rankH'=k+t로 되는 것(선형 독립인 것)」, 「패리티 검사 행렬 H'이 본래의 패리티 검사 행렬 H를 유지하는 것」과 같은 구속 조건 하에서, 상기 도 3에 나타내는 방법 또는 그것과는 다른 기지의 방법에 의해 생성한다. 또, t의 사이즈는, 시스템의 요구 조건에 의존한다. 또한, 상기 t 열분의 0행렬은, 상기 구속 조건을 만족시킬 수 있는 것이면, 반드시 0행렬일 필요는 없다.

또한, 신드롬 요구를 수취한(단계 S5, 아니오) 송신측의 통신 장치의 패리티 검사 행렬 생성부(10)에 있어서도, 상기와 동일한 처리로, 패리티 검사 행렬 H를 유지한 상태로 t 행분의 행렬 H'''을 추가 생성하고(도 9 참조), 그 후, 본래의 패리티 검사 행렬 H와 t 열분의 0행렬과 상기 행렬 H'''를 조합한 행렬 H'로부터 「H'G'=0」를 만족시키는 생성 행렬 G', G^{-1}(G^{-1}·G'=I:단위행렬)을 생성한다(단계 S7).

다음에, 송신측의 통신 장치에서는, 신드롬 생성부(14)가, 단계 S3의 처리로 메모리 등에 보존되어 있는 t 비트분의 송신 데이터 m_A'를 판독하고, 당해 송신 데이터 m_A'와 송신 데이터 m_A와 패리티 검사 행렬 H'을 이용하여 도 9에 나타내는 t 행분의 신드롬 S_A'를 계산하고, 그 결과를, 공개 통신로 통신부(13), 공개 통신로를 거쳐 수신측의 통신 장치에 통지한다(단계 S8). 그리고, 수신측의 통신 장치에서는, 공개 통신로 통신부(34)에 의해 t 행분의 신드롬 S_A'를 수신하고, 그것을 신드롬 복호부(33)에 통지한다(단계 S19). 또, 이 단계에서, 신드롬 S_A'(t 비트분의 정보)는 도청자에게 알려질 가능성이 있다.

다음에, 신드롬 복호부(33)에서는, 단계 S13의 처리에서 메모리 등에 보존되어 있는 t 비트분의 수신 데이터 m_B'을 판독하고, 기지의 신드롬 복호법을 이용하여, 확률 정보 첨부의 경 판정값 m_B과 수신 데이터 m_B'의 오류를 정정하며, 본래의 송신 데이터 m_A와 송신 데이터 m_A'를 추정한다(단계 S15). 본 실시예에서는, 예컨대, 「$(S_A+S_A')=H'm_C$」을 만족시키는 m_C를 확률 정보 첨부의 경 판정값 m_B와 수신 데이터 m_B'로부터 추정하고, 그 추정 결과 m_C를 공유 정보 m_A로 한다.

이후, 본 실시예의 수신측의 통신 장치에 있어서는, 단계 S15의 처리에 의해 경 판정값 m_B의 오류를 완전히 정정할 수 있을 때까지, 패리티 검사 행렬의 행수 및 열수를 증가시키면서 단계 S17-S19의 처리를 반복하여 실행하고, 오류를 완전히 정정할 수 있었던 단계에서, 공유키 생성부(35)가, 공개된 오류 정정 정보(예컨대, 도청되었을 가능성이 있는 상기 k+t 비트분의 정보: S_A+S_A'(도 9 참조))에 따라 공유 정보(m_A+m_A')의 일부를 버려, 항상 일정한 n-k 비트분의 정보량을 갖춘 암호키 r을 생성한다(단계 S16). 수신측의 통신 장치는, 이 암호키 r을 송신측의 통신 장치와의 공유키로 한다.

또한, 본 실시예의 송신측의 통신 장치에 있어서는, 새로운 신드롬 요구가 통지되지 않을 때까지, 패리티 검사 행렬의 행수 및 열수를 증가시키면서 단계 S7, S8의 처리를 반복하여 실행하고, 새로운 신드롬 요구가 통지되지 않은 단계에서, 공유키 생성부(15)가, 공개된 오류 정정 정보(예컨대, 도청되었을 가능성이 있는 상기 k+t 비트분의 정보: S_A+S_A'(도 9 참조))에 따라 공유 정보(m_A+m_A')의 일부를 버려, 항상 일정한 n-k 비트분의 정보량을 갖춘 암호키 r을 생성한다(단계 S6). 송신측의 통신 장치는, 이 암호키 r을 수신측의 통신 장치와의 공유키로 한다.

이와 같이, 본 실시예에 있어서는, 수신 데이터의 오류를 완전히 정정할 수 있을 때까지, 소정의 구속 조건 하에서 패리티 검사 행렬의 행수 및 열수를 증가시키면서, 오류 정정 처리를 반복하여 실행하는 구성으로 했다. 이에 따라, 통신로의 잡음 레벨을 어림하기 위해 생성한 공유 정보를 파기할 필요가 없어지기 때문에, 공유키의 생성 효율을 대폭 향상시킬 수 있다. 또한, 항상 일정한 정보량을 갖춘 암호키를 얻을 수 있다.

이상, 설명한 바와 같이, 본 발명에 의하면, 확정적인 패리티 검사 행렬을 이용하여 수신 데이터의 오류를 정정하고, 공개된 오류 정정 정보에 따라 공유 정보의 일부를 버리는 구성으로 했다. 이에 따라, 오류 비트를 특정/정정하기 위한 방대한 회수의 패리티의 교환이 없어지기 때문에, 오류 정정 처리에 걸리는 시간을 대폭 단축 가능하다는 효과를 나타낸다. 또한, 공개된 정보에 따라 공유 정보의 일부를 버리고 있기 때문에, 고도로 안전성이 보증된 공통키를 생성할 수 있다는 효과를 나타낸다. 또한, 수신 데이터의 오류를 완전히 정정할 수 있을 때까지, 소정의 구속 조건 하에서 패리티 검사 행렬의 행수를 증가시키면서, 오류 정정 처리를 반복하여 실행하는 구성으로 했다. 이에 따라, 통신로의 잡음 레벨을 어림하기 위해 생성한 공유 정보를 파기할 필요가 없어지기 때문에, 공유키의 생성 효율을 대폭 향상시킬 수 있다는 효과를 나타낸다.

산업상 이용 가능성

이상과 같이, 본 발명에 따른 양자키 배송 방법 및 통신 장치는, 고도로 안전성이 보증된 공통키를 생성하는 기술로서 유용하며, 특히, 도청자가 존재할 가능성이 있는 전송로 상의 통신에 적합하다.

청구의 범위

청구항 1.

양자 통신로 상의 광자의 측정 결과로서 얻어지는 확률 정보 첨부 수신 데이터의 오류를 정정함으로써 본래의 송신 데이터를 추정하고, 그 추정 결과를 공유 정보로 하는 양자키 배송 방법에 있어서,

송신측 및 수신측의 통신 장치가, 개별적으로 제 1 패리티 검사 행렬(요소가 「0」 또는 「1」의 동일한 행렬)을 생성하는 제 1 검사 행렬 생성 단계와,

상기 송신측의 통신 장치가, 상기 제 1 패리티 검사 행렬과 상기 송신 데이터에 근거하여 생성한 제 1 오류 정정 정보를, 공개 통신로를 거쳐서 상기 수신측의 통신 장치에 통지하는 제 1 오류 정정 정보 통지 단계와,

상기 수신측의 통신 장치가, 상기 제 1 오류 정정 정보에 근거하여 상기 수신 데이터의 오류를 정정하는 제 1 오류 정정 단계와,

상기 수신 데이터의 오류를 완전히 정정할 수 없던 경우에, 수신측 및 송신측의 통신 장치가, 전회의 오류 정정 정보가 다음 오류 정정시의 정보의 일부가 되도록, 개별적으로 제 2 패리티 검사 행렬(요소가 「0」 또는 「1」의 동일한 행렬)을 생성하는 제 2 검사 행렬 생성 단계와,

상기 송신측의 통신 장치가, 상기 제 2 패리티 검사 행렬과 상기 송신 데이터에 근거하여 생성한 추가분의 제 2 오류 정정 정보를, 공개 통신로를 거쳐서 상기 수신측의 통신 장치에 통지하는 제 2 오류 정정 정보 통지 단계와,

상기 수신측의 통신 장치가, 상기 제 1 및 제 2 오류 정정 정보에 근거하여 상기 수신 데이터의 오류를 정정하는 제 2 오류 정정 단계와,

상기 제 1 오류 정정 단계의 처리에서 수신 데이터의 오류를 완전히 정정할 수 있었던 경우, 또는, 상기 제 2 검사 행렬 생성 단계, 상기 제 2 오류 정정 정보 통지 단계, 상기 제 2 오류 정정 단계의 처리를 반복하여 실행함으로써 오류를 완전히 정정할 수 있었던 경우, 공개된 오류 정정 정보량에 따라 공유 정보의 일부를 파기하고, 그 결과를 암호키로 하는 암호키 생성 단계

를 포함하는 것을 특징으로 하는 양자키 배송 방법.

청구항 2.

제 1 항에 있어서,

상기 제 2 검사 행렬 생성 단계에서는,

「전회의 오류 정정 정보가 다음 오류 정정시의 정보의 일부로 되는 것」, 「제 1 패리티 검사 행렬의 열수=제 2 패리티 검사 행렬의 열수」, 「제 1 패리티 검사 행렬의 행수<제 2 패리티 검사 행렬의 행수」와 같은 구속 조건 하에서, 상기 제 1 패리티 검사 행렬을 포함하지 않는 새로운 제 2 패리티 검사 행렬을 생성하는 것을 특징으로 하는 양자키 배송 방법.

청구항 3.

제 1 항에 있어서,

상기 제 2 검사 행렬 생성 단계에서는,

「전회의 오류 정정 정보가 다음 오류 정정시의 정보의 일부로 되는 것」, 「선형 독립인 것」, 「제 1 패리티 검사 행렬을 포함하는 것」, 「제 1 패리티 검사 행렬의 열수=제 2 패리티 검사 행렬의 열수」, 「제 1 패리티 검사 행렬의 행수<제 2 패리티 검사 행렬의 행수」와 같은 구속 조건 하에서, 상기 제 1 패리티 검사 행렬을 포함하는 제 2 패리티 검사 행렬을 생성하는 것을 특징으로 하는 양자키 배송 방법.

청구항 4.

제 1 항에 있어서,

상기 제 2 검사 행렬 생성 단계에서는,

「전회의 오류 정정 정보가 다음 오류 정정시의 정보의 일부로 되는 것」, 「선형 독립인 것」, 「제 1 패리티 검사 행렬을 포함하는 것」, 「제 1 패리티 검사 행렬의 열수<제 2 패리티 검사 행렬의 열수」, 「제 1 패리티 검사 행렬의 행수<제 2 패리티 검사 행렬의 행수」와 같은 구속 조건 하에서, 상기 제 1 패리티 검사 행렬을 포함하는 제 2 패리티 검사 행렬을 생성하고,

상기 제 2 오류 정정 정보 통지 단계에서는,

상기 제 2 패리티 검사 행렬과 상기 송신 데이터와, 또한 상기 제 2 패리티 검사 행렬의 열수 증가분에 따라 추가되는 송신 데이터에 근거하여, 상기 제 2 오류 정정 정보를 생성하고, 그 생성 결과를, 공개 통신로를 거쳐서 상기 수신측의 통신 장치에 통지하고,

상기 제 2 오류 정정 단계에서는,

상기 제 1 및 제 2 오류 정정 정보에 근거하여, 상기 수신 데이터의 오류와 상기 추가 송신 데이터에 대응하는 수신 데이터의 오류를 정정하는

것을 특징으로 하는 양자키 배송 방법.

청구항 5.

양자 통신로 상의 광자의 측정 결과로서 얻어지는 확률 정보 첨부 수신 데이터의 오류를 정정함으로써 본래의 송신 데이터를 추정하고, 그 추정 결과를 송신측의 통신 장치와의 공유 정보로 하는 수신측의 통신 장치에 있어서,

미리 생성해 놓은 송신측의 통신 장치와 동일한 제 1 패리티 검사 행렬(요소가 「0」 또는 「1」의 행렬), 상기 송신측의 통신 장치로부터 공개 통신로를 거쳐서 수취한 상기 제 1 패리티 검사 행렬과 상기 송신 데이터에 근거한 제 1 오류 정정 정보에 근거하여, 상기 수신 데이터의 오류를 정정하는 제 1 복호 수단과,

상기 수신 데이터의 오류를 완전히 정정할 수 없었던 경우에, 전회의 오류 정정 정보가 다음 오류 정정시의 정보의 일부가 되도록, 송신측의 통신 장치와 동일한 제 2 패리티 검사 행렬(요소가 「0」 또는 「1」의 행렬)을 생성하고, 그 후, 상기 제 1 오류 정정 정보, 및 상기 제 2 패리티 검사 행렬의 생성에 의해 추가되는 제 2 오류 정정 정보에 근거하여, 상기 수신 데이터의 오류를 정정하는 제 2 복호 수단과,

수신 데이터의 오류를 완전히 정정할 수 있었던 경우에, 공개된 오류 정정 정보량에 따라 공유 정보의 일부를 파기하고, 그 결과를 암호키로 하는 암호키 생성 수단

을 구비하는 것을 특징으로 하는 통신 장치.

청구항 6.

수신측의 통신 장치가 양자 통신로 상의 광자의 측정 결과로서 얻어지는 확률 정보 첨부 수신 데이터로부터 본래의 송신 데이터를 추정한 경우에, 그 추정 결과를 수신측의 통신 장치와의 공유 정보로 하는 송신측의 통신 장치에 있어서,

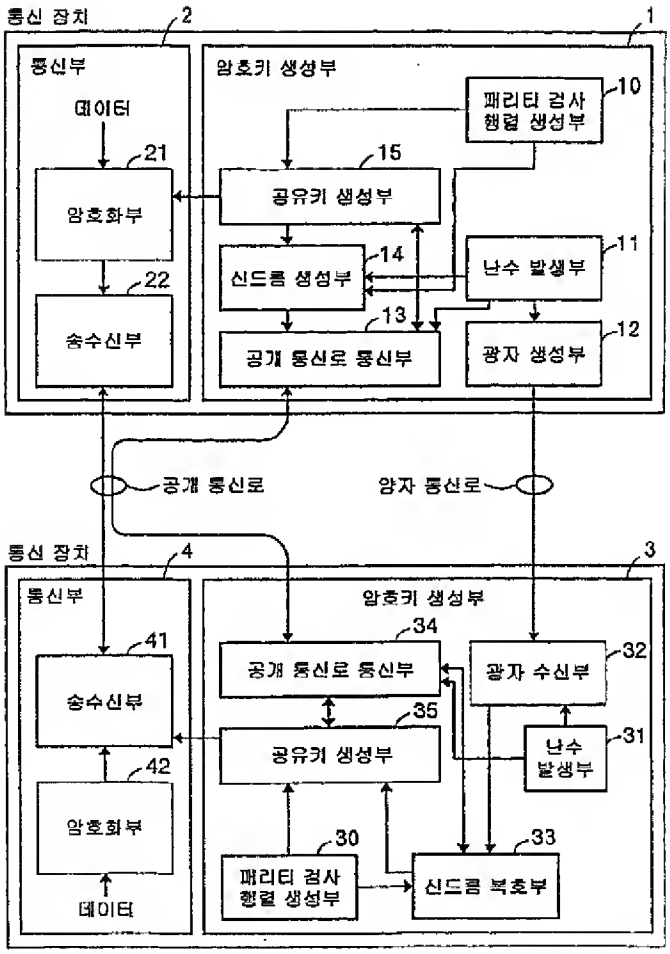
미리 생성해 놓은 제 1 패리티 검사 행렬과 상기 송신 데이터에 근거하여 제 1 오류 정정 정보를 생성하고, 그 생성 결과를, 공개 통신로를 거쳐서 상기 수신측의 통신 장치에 통지하는 제 1 오류 정정 정보 생성 수단과,

상기 수신측의 통신 장치에 의해 수신 데이터의 오류를 완전히 정정할 수 없던 경우에, 전회의 오류 정정 정보가 다음 오류 정정시의 정보의 일부가 되도록, 상기 수신측의 통신 장치와 동일한 제 2 패리티 검사 행렬(요소가 「0」 또는 「1」의 행렬)을 생성하고, 그 후, 상기 제 2 패리티 검사 행렬과 상기 송신 데이터에 근거하여 생성한 추가분의 제 2 오류 정정 정보를, 공개 통신로를 거쳐서 상기 수신측의 통신 장치에 통지하는 제 2 오류 정정 정보 생성 수단과,

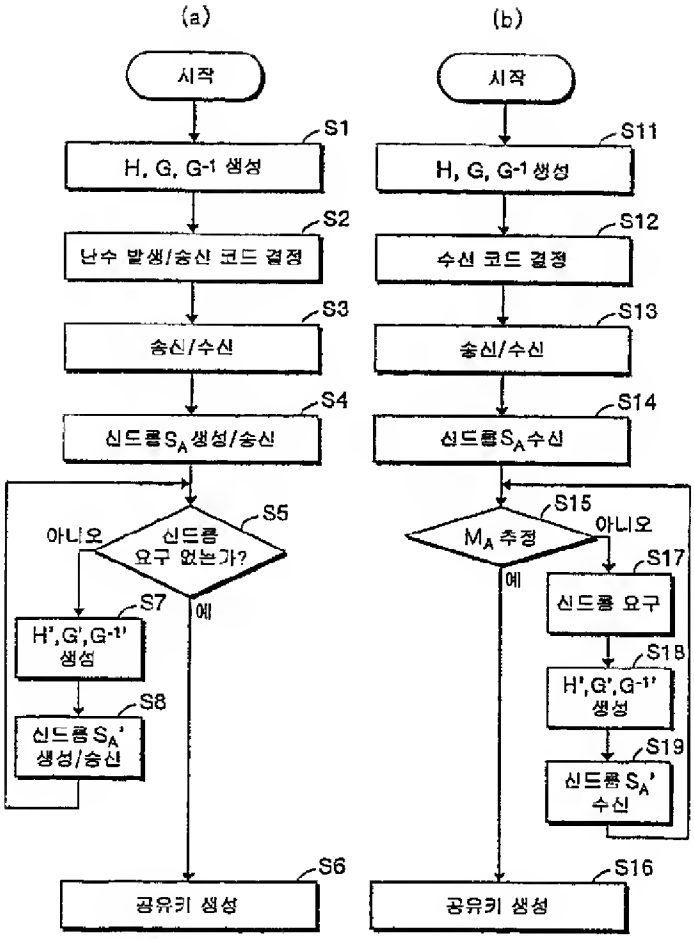
상기 수신측의 통신 장치에 의해 수신 데이터의 오류를 완전히 정정할 수 있었던 경우에, 공개한 오류 정정 정보량에 따라 공유 정보의 일부를 파기하고, 그 결과를 암호키로 하는 암호키 생성 수단

을 구비하는 것을 특징으로 하는 통신 장치.

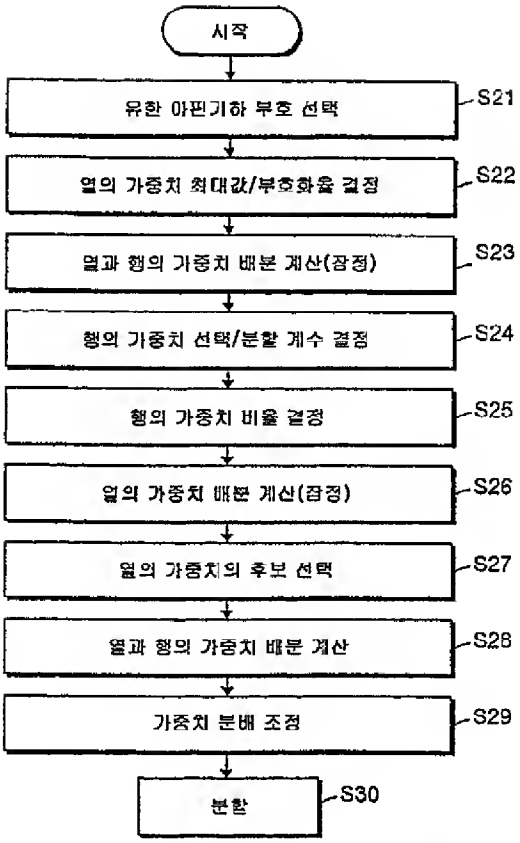
도면1


통신 장치
2
1
통신부
암호키 생성부
데이터
패리티 검사 행렬 생성부
10
21
15
암호화부
공유키 생성부
14
11
신드롬 생성부
난수 발생부
22
13
12
송수신부
공개 통신로 통신부
광자 생성부
공개 통신로
암자 통신로
통신 장치
4
3
통신부
암호키 생성부
34
41
32
공개 통신로 통신부
광자 수신부
35
송수신부
난수 발생부
31
공유키 생성부
42
암호화부
30
33
패리티 검사 행렬 생성부
신드롬 복호부
데이터

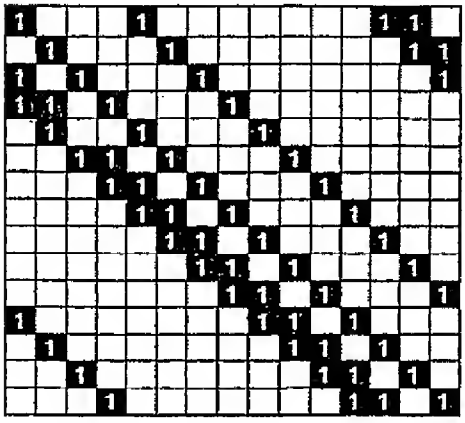
도면2


(a)
시작
S1
H, G, G-1 생성
S2
난수 발생/송신 코드 결정
S3
송신/수신
S4
신드롬 S_A 생성/송신
S5
신드롬 요구 없는가?
아니오
예
S7
H', G', G-1' 생성
S8
신드롬 S_A' 생성/송신
S6
공유키 생성
(b)
시작
S11
H, G, G-1 생성
S12
수신 코드 결정
S13
송신/수신
S14
신드롬 S_A 수신
S15
M_A 추정
아니오
예
S17
신드롬 요구
S18
H', G', G-1' 생성
S19
신드롬 S_A' 수신
S16
공유키 생성

도면3


시작
유한 아핀기하 부호 선택
S21
열의 가중치 최대값/부호화율 결정
S22
열과 행의 가중치 배분 계산(잠정)
S23
행의 가중치 선택/분할 계수 결정
S24
행의 가중치 비율 결정
S25
열의 가중치 배분 계산(잠정)
S26
열의 가중치의 후보 선택
S27
열과 행의 가중치 배분 계산
S28
가중치 분배 조정
S29
분할
S30

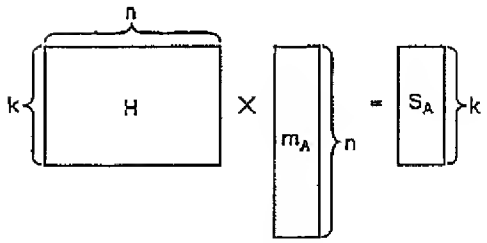
도면4



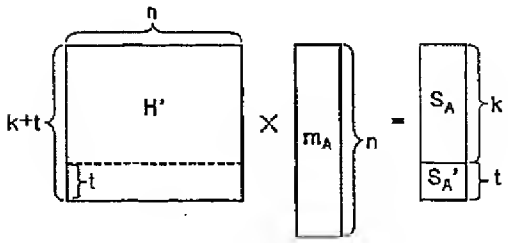
도면5

레이트		0.5	
N		12.6	
l	γ_l	$\lambda(\gamma_l)$	$n(\gamma_l)$
1	2	0.27381	69
2	3	0.10714	18
3	8	0.61905	39
u		ρ_u	n_u
8		1	63

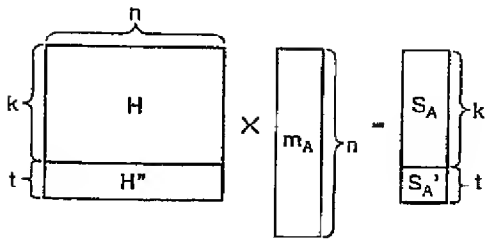
도면6



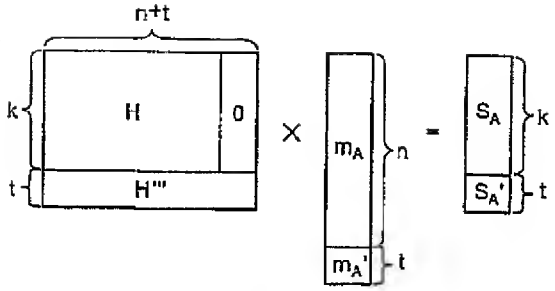
도면7



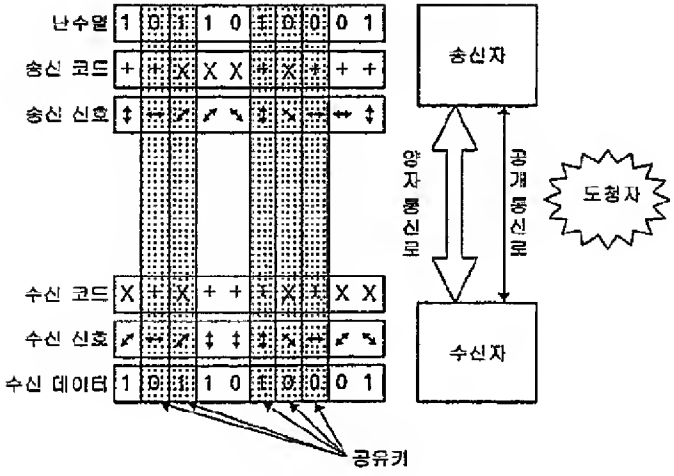
도면8



도면9


n+t
k
H
0
t
H'''
×
m_A
n
m_A'
t
=
S_A
k
S_A'
t

도면10


난수열
송신 코드
송신 신호
수신 코드
수신 신호
수신 데이터
송신자
양자 통신로
공개 통신로
도청자
수신자
공유키